5160 Decarie Boulevard, Suite 502
Montreal, QC, H3X 2H9 Canada
1 (800) 585-9694

Security Information Package

Online Voting Security for the 2022 Ontario Municipal Elections

Security Overview

Simply Voting Inc. will be providing the Internet and Telephone Voting System for the 2022 Ontario Municipal Elections. The Simply Voting system is secure and protects the secrecy of your vote.

Secret Ballot

Whether you use the internet or telephone to vote, your vote is instantly encrypted and stored with no possibility of your vote being traced back to your identity, just like a traditional paper ballot.
It is impossible for municipal staff, Simply Voting employees or any other person to see how you have voted. Election officials will only be able to see that you cast your vote, the time you voted and the IP address or telephone number you voted from.

One Person One Vote

Only registered voters on the municipal list of electors will be authorized to access a ballot. Once you vote, using either internet or telephone, you are “crossed off” the list and cannot vote again. Even if you switch between the internet and telephone, even if you try to vote using several devices at the same time, the system will only accept one single ballot from each voter.

Auditing

Municipalities will assign independent auditors of the Internet and Telephone Voting System. Simply Voting provides designated auditors with appropriate access to observe that the system allows voting under proper circumstances and prohibits voting under improper circumstances. The Auditor may continuously monitor voting activity before, during and after the voting period. It is also impossible for the Auditor to see how you have voted.

For some municipalities: Once your vote is cast a receipt code is issued. Only you will know this code. Print this code or write it down. After voting has ended, you can look up your receipt code to verify that your vote was counted.

Protection Against Computer Hackers

Simply Voting is an expert in internet security and goes to great lengths to protect the voting system. All communications between your computer and the voting website are encrypted to ensure confidentiality. The internet ballot is tamperproof and there are multiple layers of security to protect the servers against attacks.

Protection Against Imposters

To vote, you will need to enter a password. Every password is a nine-digit numeric PIN that will be mailed to each voter in a Voter Information Letter prior to the "Voting Period". These PINs are randomly generated by Simply Voting and are printed, machine folded in security-tinted envelopes, and mailed directly to voters using Canada Post. As an added security measure, voters will also be required to enter their date of birth to complete the voting procedure. Therefore, if your Voter Information Letter ends up in the wrong hands, another person will not be able to cast your vote without your PIN and your date of birth.

Technical Information

Top-Notch Security

Simply Voting was designed from the ground-up to minimize the risk of electoral fraud or breach of secrecy:

- Voters who bypass authentication or have already voted are denied access to the ballot.
- One-vote-per-voter is guaranteed by marking electors as voted and storing the vote in a single transaction. Even if a voter submits the ballot simultaneously on several devices, this technology guarantees that only one vote is accepted.
- Ballots are rigorously checked for validity before being accepted.
- All administrator and voter activity is logged with timestamp and IP address.
- Communication between the voter's computer and our website is encrypted with TLS 1.2 and strong cipher suites to protect against current and future encryption attacks.
- The entire voting system database is encrypted at rest using AES-256 encryption.
- Our servers are "hardened" and are subjected to daily Trust Guard PCI Compliance security scans.
- Our voting system is regularly subjected to penetration tests by CyberHunter and source code security audits by HP Fortify.
- Simply Voting adheres to guidelines established by the Open Web Application Security Project.
- Any change to the voting system must pass an internal security review before going live.
- All staff workstations are kept up-to-date and protected by access password, firewall, anti-virus, anti-spamware and disk encryption.
- We authenticate our emails with DomainKeys Identified Mail and the Sender Policy Framework to protect voters from phishing attacks.
- Our servers are protected by a very powerful firewall, FortiGate Unified Threat Management, which includes an Intrusion Detection System and a redundant firewall on hot standby.
- Network access is protected by a Virtual Private Network (VPN) and Two-Factor Authentication (2FA).
- Simply Voting uses an automated and always-on solution from Radware to protect against Denial of Service (DoS) attacks.
- We use redundant Anycast DNS deployments which protects against DNS-based DoS attacks.

Fully Hosted & Reliable

Simply Voting is built on an enterprise-class cloud computing service powered by high performance IBM hardware, with full redundancy across the entire infrastructure (no single points of failure). Our data centre is in a stable mountain zone, away from earthquake, hurricane, tornado, and severe weather zones. The data center contains advanced power, cooling and security infrastructure, and Cisco Data Center 3.0 network architecture. It is staffed 24x7, backed-up by an offsite network operations center. We also use several Anycast DNS clusters to ensure fault tolerance at the DNS level.

Simply Voting uses third party offsite monitoring tools to automatically monitor key “vital signs” of our voting system 24x7 and a technical staff member is immediately notified of any anomaly. Simply Voting maintains a Disaster Recovery Plan as well as a Hot Site at a backup data center in a different geographical area. The Hot Site is synchronized with the primary data center using remote database replication. Should the primary data center experience an outage, we have the capability of quickly redirecting traffic of the entire voting system to the Hot Site, minimizing disruption to ongoing elections and avoiding any loss of data. You can rest assured that your election is always protected and available in the case of a disaster.

For telephone voting, Simply Voting uses industry leader Plum Voice as a voice-to-web interface layered on top of our online voting system. Every component in the Plum Voice, fault-tolerant infrastructure has a backup and Plum's platforms have been tested by billions of calls since 2000. Plum's PCI Level 1 compliant operation actively secures and protects applications and data from digital, physical, and social intrusion vectors. Thanks to Plum Voice's flexible technology Simply Voting can easily scale up or down the number of dedicated ports needed, and the telephone voting system can handle spikes well beyond that number.

Confidentiality

Simply Voting takes secrecy of the vote very seriously. It is impossible for election organizers to determine what a particular voter has voted as the results are anonymous. All voter information is removed from our servers if you choose to have the election deleted. We never make use of voter information for anything other than voting and never share such information with third parties. Our privacy policy (available on the Simply Voting website) and voting system have been independently certified by TRUSTe for compliance with their Privacy Certification and Trusted Cloud requirements.

TRUSTe
CERTIFIED PRIVACY

McAfee Enterprise-Ready Rating

Simply Voting received the highest CloudTrust Rating from McAfee. McAfee performs objective and thorough evaluations of cloud services based on a detailed set of criteria developed in conjunction with the Cloud Security Alliance (CSA). Services designated as McAfee Enterprise-Ready fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection.

McAfee™
ENTERPRISE-READY

SOC 2 Compliance

Simply Voting is SOC 2 Type 1 compliant. The SOC 2 is a widely recognized auditing standard issued by the American Institute of Certified Public Accountants (AICPA). An auditor's report details a service provider's ability to offer adequate controls and safeguards when they host or process data belonging to their customers. The audit focuses heavily in the areas of security, availability and confidentiality. It addresses important topics such as backup and recovery, computer operations, and human resources. The data centers where Simply Voting servers are located are similarly SOC 2 Type 2 compliant. These attestations are an independent validation of the quality, integrity and reliability of Simply Voting's infrastructure and services.

Advanced DDoS Protection Service

With Radware

Denial-of-service (DoS) attacks are on the rise and have evolved into complex and overwhelming security challenges for organizations large and small. Although DoS attacks are not a recent phenomenon, the methods and resources available to conduct and mask such attacks have dramatically evolved to include distributed (DDoS) and, more recently, distributed reflector (DRDoS) attacks.

Radware's DDoS protection service monitors all traffic entering its network for large-volume floods that aim to disrupt the services. Features of this best-in-class protection include behavioral-based detection using advanced, patented machine learning algorithms to protect against known and unknown threats; protection against network and application-layer DDoS attacks, protection against encrypted flood attacks without requiring customers to provide decryption keys and without adding latency in peacetime, as well as extensive compliance options and certifications, unparalleled by any rival, including industry-specific certifications such as PCI and HIPAA, as well as cloud security standards such as SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018, ISO 27032, etc.

Simply Voting enjoys the protection of an always-on solution that combines Radware's DefensePro attack mitigation appliances with their Cloud DDoS Protection Service. The DefensePro locally filters all traffic entering Simply Voting's private cloud infrastructure hosted at Terago data centres. If additional mitigation capacity is needed the DefensePro automatically triggers a redirection of traffic to Radware's cloud-based scrubbing centres. This hybrid solution leverages the real-time protection and minimal latency of an on-premise solution with the massive capacity of a cloud service that is activated on demand.

The Data Centres

TeraGo

Secure and Reliable

- Multi-factor access authentication with monitoring and surveillance
- Ultra redundant mechanical and electrical infrastructure
- 24/7 monitoring by two geo-redundant Canadian Network Operations Centres

Best Practice Standards

- Meets governance standards
- Follows ITIL service management methodology with certified staff
- Redundant infrastructure and 24/7 monitoring

Enterprise Disaster Recovery

- Data located in Canada
- Multiple location options for secondary site geo-redundancy
- Flexible capacity

Facilities

TeraGo owns and operates five data centres across Canada. Below are additional details about their flagship data centres located in Kelowna, British Columbia and Mississauga, Ontario, used by Simply Voting Inc.

Category	Kelowna, BC	Mississauga, ON
Designed to DC Tier	Tier III	Tier III
Power Redundancy	2N	2N + 1
Max Power Density	Up to 5 kVa	Up to 18 kVa
Backup Generator Capacity	> 48 hours at full load – across all facilities	
DC Network Connectivity	10 Gbps +	10 Gbps +
Carrier Redundancy	Multiple Tier 1 providers	Multiple Tier 1 providers
TeraGo Hybrid Cloud Capable	Yes	Yes
Compliance	AT101 SOC Type II and SSAE 16 – across all facilities	
Security	24/7 security and video monitoring, multi-factor biometric access authentication, man traps, proximity scanners	
Support	24x7x365 support	

Kelowna, BC:

- Strategically situated in one of North America's lowest risk profile locations
- Unique Gigavault design, with hard walled enclosures providing segregated and secured spaces
- Carrier neutral facility with diverse connectivity from multiple providers
- Green energy efficient facility design with cold aisle containment and air cooling during winter
- Design to Uptime Institute Tier III specifications, including 2N+1 redundant power infrastructure from ring bus substations

Mississauga, ON:

- State of the art facility in the greater Toronto area
- Over 1 MW of total IT critical power capacity
- Carrier neutral facility with diverse connectivity and with direct connectivity to 151 Front
- Design to Uptime Institute Tier III specifications, including utility feed from 2 substations and 2N power architecture

For more information, please write to info@simplyvoting.com